Annex 22 - Information and Cyber Security

Primary Agency: Department of Innovation & Technology (DoIT)

Supporting Agencies: Illinois State Police (ISP)
Illinois Emergency Management Agency (IEMA)
Illinois National Guard (ILNG)
Illinois Attorney General's Office (OAG)
Statewide Terrorism and Intelligence Center (STIC)

I. Purpose

A. Provide strategic and operational guidance to organizations on coordinated incident handling of threats and events that involve information technology (IT) systems and assets of the state and that impact critical and lifeline infrastructure, the environment and public safety.

B. Scope

1. This annex addresses cyber or physical threats and/or incidents that have a disruptive impact on critical services.

2. This annex is only applicable to state supported information technology systems and assets.

3. This annex supplements policies and procedures contained in the Illinois Emergency Operations Plan (IEOP) and may be implemented independent of other planning documents.

4. This annex does not provide handling procedures for all potential incidents affecting IT systems and assets.

5. Laws, rules, regulations and policies of the United States government and agencies involved in risk management, assessment, protective measures and prevention activities for IT are considered valid and/or applicable within the state of Illinois.

6. For the purposes of this annex, incident handling refers to the overall process of detection, reporting, analysis, incident containment, response, recovery and notification of others to mitigate violations of security policies and recommended practices, acceptable use policies or standard security practices.

7. For the purposes of this annex, clarifying definitions are provided in IEOP Annex 22 A-1, Glossary.

C. Policy

1. Procedures for utilization, control and use will incorporate and/or consider operational priorities that include, but are not limited to, the protection of life, public health and safety, property protection, environmental protection, restoration of essential utilities, restoration of essential program functions and coordination as appropriate.

2. The governor or designee may authorize and direct the use of state resources to provide support and assistance to IT incident handling efforts for internal and external organizations after consideration of both priority of need and cost.

3. In situations where an imminent threat exists to life safety, or an identified need for the protection of critical infrastructure and environment exists, priorities established within the IEOP take precedence over agency priorities.

D. Situation Overview

1. An incident or threat of an incident has occurred with the potential to impact IT systems and assets of state government resulting in consequences to critical resources, networks, and systems or information that is processed, stored or transmitted, requiring prevention, protection, response, recovery and/or mitigation activities.

2. Interruptions in essential services and processes provided through critical infrastructure sectors cause imminent life safety situations and/or significant economic loss.

E. Assumptions

1. Cyber incidents will take many forms, including accidental, malicious and physical occurrences.

2. Large-scale cyber incidents will overwhelm government and private-sector resources.

3. Complications from disruptions in information and services provided through IT and cyber systems, networks and infrastructure will threaten lives, property, the economy and the public and private sectors' ability to deliver life safety and life essential services.

4. Cyber incidents will have national consequences.

5. Rapid identification, information exchange, investigation and coordinated incident handling and remediation will limit and mitigate the damage caused by the threat or actual occurrence of a significant cyber incident.

6. Delays in recognition or incident handling will increase potential consequences.

7. Delays in the coordination, dissemination and communication of cyber incident handling actions will increase potential consequences.

8. State agencies operating under the authority of constitutional officers will cooperate and coordinate incident handling with DoIT and/or the State Emergency Operations Center (SEOC) as appropriate.

II. Concept of Operations

A. General

1. Support for incident handling is coordinated through resources assigned to state agencies; however, external organizations are utilized on a routine basis through established contractual services.

2. The Department of Innovation & Technology will coordinate and manage incident handling for cyber assets and implement prevention and protection protocols for state agencies.

3. For situations not requiring activation of the SEOC, DoIT will serve as the single point of coordination for joint information, rumor control and the dissemination of cyber-related alerts, warnings and public information.

4. The Illinois Emergency Management Agency will coordinate state consequence management activities through the State Emergency Operations Center.

    a. For the purposes of the IEOP, consequence management includes but is not limited to actions and measures to protect public health and safety, restore essential government services, and provide emergency relief to governments, businesses and individuals affected by an incident.

    b. For the purposes of joint information, rumor control and the dissemination of state-wide alerts, warnings and public information the SEOC, upon activation, will serve as the single point of coordination.

5. The Illinois State Police will coordinate and manage law enforcement activities including, but not limited to, prevention, protection, investigation, evidence collection and adjudication of cyber incidents.

6. The Illinois Attorney General’s Office will coordinate with the appropriate prosecuting authorities in the prosecution of cybercrimes and assist in investigatory efforts of state agencies and external organizations.

7. The Illinois National Guard will assist in the analysis of incident intelligence, development of situational awareness, and technical assistance to prevent, protect, respond to, recover from and mitigate the effects of a cyber incident.

B. Supporting Sections

1. Notifications, Alerts and Warnings (NAW)

a) Notification to state agencies regarding cyber incidents will be carried out in accordance with Department of Innovation & Technology Computer Security Incident Response Plan (CSIRP).

b) DoIT will notify the IEMA SEOC manager and Statewide Terrorism Intelligence Center Watch Center of a cyber incident requiring notifications, alerts and/or warnings to stakeholders, key-decision makers and executive officers.

1) IEMA will notify and alert agencies and organizations of implementation of the IEOP and activation of the SEOC as appropriate, in accordance with SIREN standard operating procedures (SOP).

2) IEMA will utilize the Business Emergency Operations Center (BEOC) for notifications, alerts and/or warnings to private sector partners as appropriate.

c) Primary and support agencies and organizations are responsible for internal and support partner notifications, alerts and warnings.

2. Direction and Control

a) DoIT will administer and manage the state's incident handling efforts and coordinate as appropriate with whole community partners.

b) Upon implementation of the IEOP and activation of the SEOC, the IEMA director or designee will establish strategic and operational command, coordination and control of state resources and support organizations required for consequence management in accordance with IEOP Annex 1, Direction and Control.

c) IEMA will manage and utilize the BEOC and coordinate with DoIT to receive and disseminate disaster intelligence, establish common strategic priorities, and prioritize short, intermediate and long-term activities among the SEOC and private sector organizations.

3. Reporting Requirements

a. DoIT will serve as the central point of contact for state agencies reporting of cyber incidents or intrusions.

b. As appropriate for the type, scope and magnitude of a cyber incident, DoIT will report disruptions and intrusions to

potentially affected stakeholders, key-decision makers and executive officers in accordance with DoIT CSIRP.

c. Upon activation of the SEOC, state agencies will maintain situational updates, develop required intelligence briefings, and provide critical and priority information established for cyber incidents.

4. Resource Management and Logistics

a) Resource management and logistics will be carried out in accordance with IEOP Annex 9, Resource Management.

b) Resource management includes mutual aid agreements and assistance agreements, the use of special federal and state teams, and resource mobilization protocols.

5. Federal Coordination

a) Direct coordination with federal agencies will occur through appropriate and designated agencies.

III. Roles and Responsibilities

A. Department of Innovation & Technology (DoIT)

1. Categorize cyber incidents and determine prioritization of efforts for state agencies.

2. Conduct and/or coordinate forensic analysis and attribute cyber incidents to the source, including preparation efforts necessary to prevent initial or follow-on acts and/or develop counter-options.

3. Identify, assess and prioritize risks to inform prevention and protection activities, countermeasures and investments.

4. Implement processes to prevent ongoing, additional and cascading incidents based on information obtained from intelligence, threat assessments, alert networks, surveillance programs, and internal and external stakeholders and customers.

5. Determine level of response necessary to implement appropriate courses of action.

6. Notify, activate, deploy, coordinate, implement and sustain Computer Security Incident Response Team(s) assets.

7. Notify, alert and warn state agencies, key stakeholders and executive officers of potential and realized cyber incidents.

8. Notify the SEOC manager of cyber incidents requiring notifications, alerts and/or warnings to stakeholders, key decision makers and executive officers.

9. Coordinate incident handling activities to monitor identified threats and hazards, and adjust levels of activity commensurate with the risk.

10. Assist state agencies in response to and recovery from cyber incidents.

11. Establish and disseminate cyber specific guidance and protocols to state agencies.

12. Analyze damage from cyber incidents impacting critical and lifeline infrastructure, the environment and public safety.

13. Coordinate public information and education campaigns with state agencies, key stakeholders and executive officers.

14. Coordinate with IEMA to activate a Joint Information System and establish the state Joint Information Center.

15. Coordinate with IEMA to request implementation of the IEOP and activation of the SEOC to assist in consequence management.

16. Coordinate with local units of government and/or external organizations as applicable.

17. Maintain liaison with the SEOC upon activation.

18. Request activation of ILNG Intergovernmental Agreement (IGA) or external response assets through the SEOC.

B. Illinois Emergency Management Agency (IEMA)

1. Coordinate with the DoIT liaison to determine the need to implement the IEOP and activate the SEOC for consequence management efforts.

2. Determine appropriate level of activation for the SEOC.

3. Notify agency liaisons of SEOC activation in accordance with SOPs.

4. Coordinate and manage strategic and operational command, coordination and control of state resources and support organizations required for consequence management.

5. Manage the state resource management system to address the identification, location, acquisition, storage, maintenance and testing, timely distribution and accounting for services and materials.

C. Illinois State Police (ISP)

1. Assist law enforcement having jurisdiction or investigative agencies in the forensic analysis, attribution, investigation and adjudication of cyber incidents.

2. Coordinate and manage state law enforcement activities to halt, apprehend, or secure threats and/or hazards.

3. Identify, discover or locate threats and/or hazards through active and passive surveillance and search procedures to include the use of systematic examinations and assessments, sensor technologies or physical investigation and intelligence.

4. Through the Statewide Terrorism and Intelligence Center

a. Collect, analyze and disseminate intelligence information.

b. Conduct threat and risk analyses.

c. Assist law enforcement as appropriate.

d. Maintain liaison with the SEOC upon activation.

D. Illinois Attorney General's Office (AGO)

1. Coordinate with appropriate prosecuting authorities for the prosecution of criminal cases brought by the state.

E. Illinois National Guard (ILNG)

1. Assist in the analysis of incident intelligence, development of situational awareness, and technical assistance to prevent, protect, respond to, recover from and mitigate the effects of a cyber incident.

2. Activate IGA for external response assets with DoIT upon request and gubernatorial approval.

IV. Authorities and References

A. Authorities

1. Illinois Emergency Operations Plan, as amended.

2. Illinois Emergency Management Act, 20 ILCS 3305 as amended.

3. State Police Act, 20 ILCS 2610

4. Attorney General Act, 15 ILCS 205

5. Executive Order 2016-01

6. State Guard Act 20 ILCS 1815

7. Department of Central Management Services Law 20 ILCS 405

8. DoIT/ILNG Intergovernmental Agreement

B. References

1. Robert T. Stafford Disaster Relief and Emergency Assistance Act, as amended, 42 U.S.C. § 5121 et seq.

2. Homeland Security Presidential Directive 12 (HSPD 12)

3. Department of Innovation & Technology Computer Security Incident Response Plan (DoIT CSIRP), as amended

4. Illinois Emergency Operations Plan Annex 27, Military Coordination.